Optical image encryption technique based on compressed sensing and Arnold transformation

Xiaoyong Liu, Yiping Cao, Pei Lu, Xi Lu, Yang Li

Opto-Electronics Department, Sichuan Unviersity, China
Key laboratory of Ecophysics and Department of Physics, College of Science, China
College of information science and technology, Shihezi university, China

Journal club presentation
Presenter: Nitin Rawat
Date: 27/02/2014

Optical image encryption technique based on compressed sensing and Arnold transform

Fig. 1 shows double random phase encoding (DPRE) technique.

- Let an image multiplied by a single random matrix $\exp[i\phi_1(x,y)]$ and further taking its Fourier transform of the result to get an encrypted image.
- Decryption process is reversed by taking the complex conjugate of the random phase and further its inverse Fourier transform.
- Here the key is formed by the combination of the transform and the random matrix.

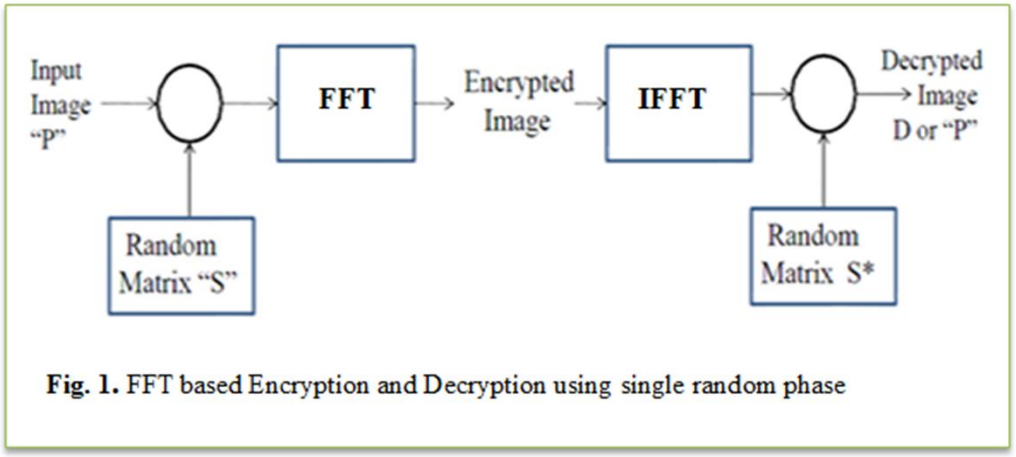

Fig. 1. FFT based Encryption and Decryption using single random phase

Optical image encryption technique based on compressed sensing and Arnold transform

Fig. 2 shows the realization of DPRE technique using a 4f system, where

$f(x,y)$ Original image

$g(x,y)$ Encrypted image

$\theta_0(x,y)$ Key function 1

$\psi_0(u,v)$ Key function 2

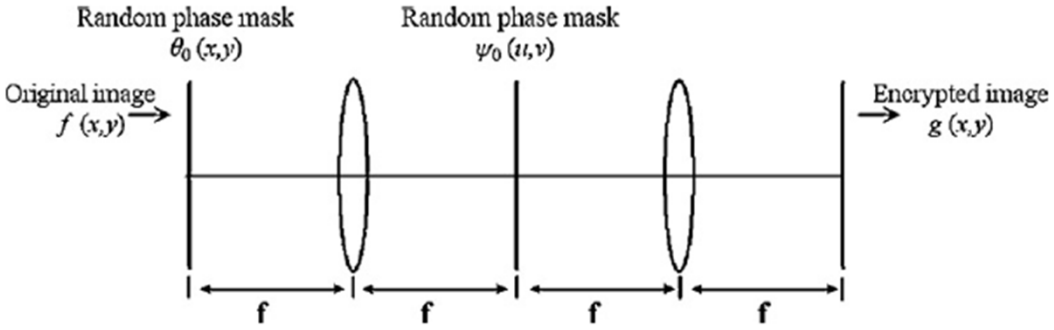

Fig. 2. Double random phase encoding (DRPE) process

The encoding process can be expressed as:

$$g(x,y) = \mathrm{FT}\left\{\mathrm{FT}\left[f(x,y)\exp[j2\pi\theta_0(x,y)]\right]\exp[j2\pi\psi_0(u,v)]\right\} \quad (1)$$

The decoding process can be expressed as:

$$f(x,y) = \mathrm{FT}^{-1}\left\{\mathrm{FT}^{-1}\left[g(x,y)\exp[-j2\pi\omega(u,v)]\right]\exp[-j2\pi\theta(x,y)]\right\} \quad (2)$$

Compressed sensing

- CS is based on the recent understanding that a small collection of measurements of a compressible signal contain enough information for reconstruction and processing.
- The process of transformation from x to y is a dimensionality reduction.
- In order to recover x from the random measurements y, the traditional method of least squares can be shown to fail with high probability.
- It has proved to use the l_1-optimization.

$$\hat{\alpha} = \arg\ \min \left\| \alpha' \right\|_1 \quad \text{s.t. } \Phi\Psi\alpha' = y$$

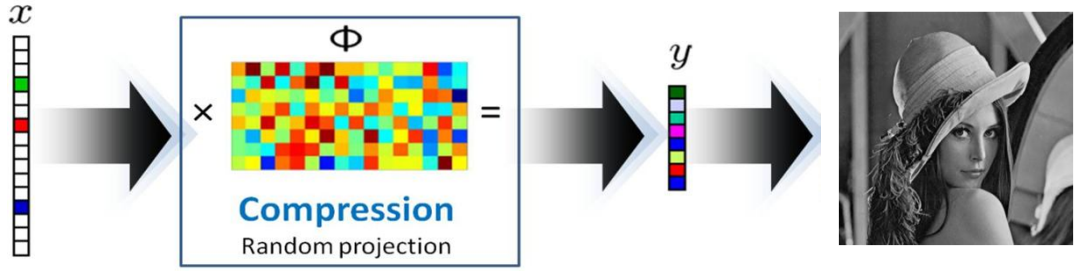

Fig. 3. Compressive sensing model shows the dimension reduction and the compression after sampling process

$$y = \Phi f = \Phi\Psi\tilde{x} \qquad (3)$$

Φ Sensing matrix, $M \times N$

$M \ll N$

$$y \longrightarrow M \times 1$$

Arnold transform

- Arnold transform (AT) is a well-known approach in the field of cryptography.
- In AT, the pixel coordinate of an image can be changed and realize image scrambling, which makes image like white noise.
- It acts as a security system key.
- Suppose that the size of an original image is $N \times N$ and (x, y) is the coordinates of the image, then (x', y') is the new coordinates of the scrambled image's pixel.

The 2-D AT is expressed as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N)$$

$$x, y \in \{0, 1, 2, ..., N-1\} \quad (4)$$

Then get the iteration process:

$$p_{ij}^{n+1} = A p_{ij}^{n} (\text{mod } N) \qquad n = 0, 1, ...$$

$$p_{ij}^{n} = (i, j) \quad \text{i,j} \in \{0, 1, 2.....N\text{-}1\} \quad (5)$$

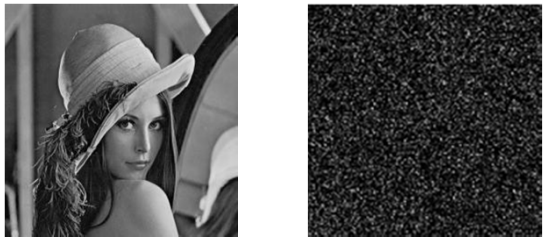

Fig. 4. Arnold transformation. (a) Original image; (b) Image after applying AT process

Optical image encryption technique based on compressed sensing and Arnold transform

Experimental results

- A few large coefficients have taken from the original image.
- Arnold transformation (AT) is used to encrypt the reduced image.
- Further DRPE technique is applied for re-encrypting the data information
- The setup is to check the object generation onto the camera.

Decoding process

- An inverse of DRPE and AT are taken.
- OMP algorithm is used to get the decrypted (original image) back.

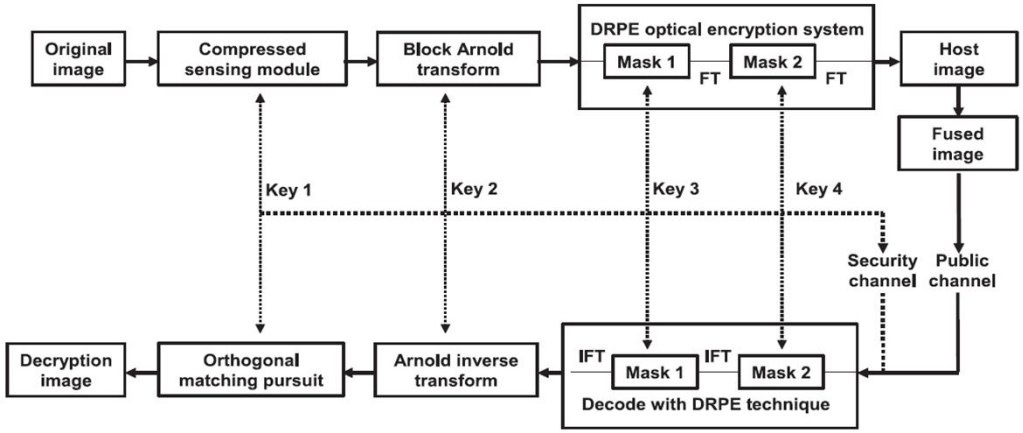

Fig. 5. The flow chart of the proposed method

Encryption-decryption results

- A grayscale image ‘peppers’ of size 256 x 256 pixels has been chosen.
- Original image is encrypted by CS.
- The random measurement matrix is used as secret key-1.
- Image is further encrypted by AT and generated scrambling image. AT acts as a secret key-2.
- Further, DRPE technique is used for re-encrypting the data information which provide a secret key-3 and key-4 (Two random phases).

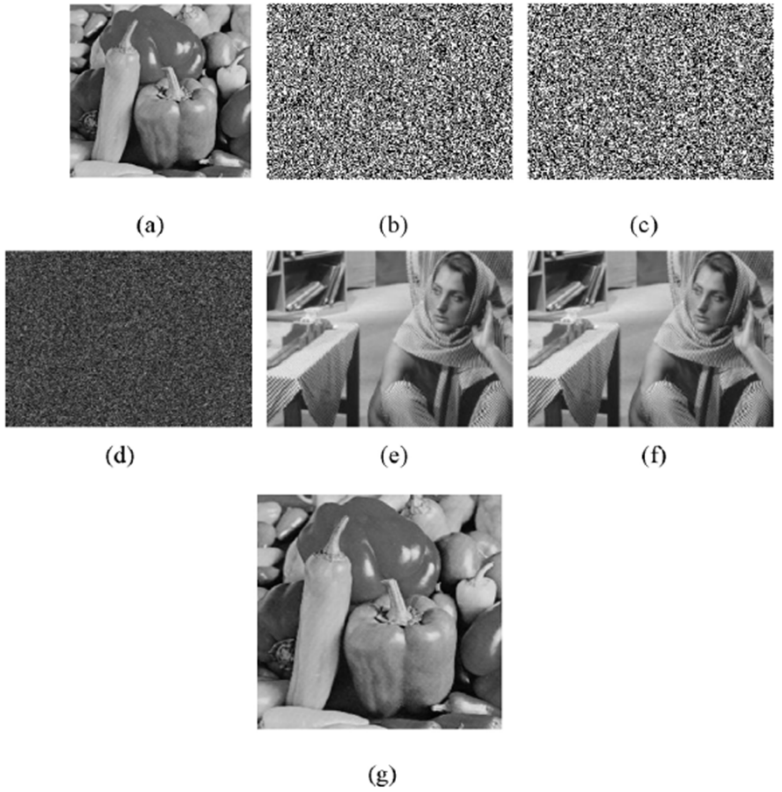

Fig. 6. Results of encryption and decryption process. (a) Original image, (b) encryption image after CS, (c) scrambling image, (d) hiding image, (e) host image, (f) fused image and (g) decryption image using right keys; PSNR = 29.3684 dB.

PSNR Analysis

Peak to peak Signal to Noise ratio

In order to verify the results of the investigation, the peak to peak signal-to-noise ratio (PSNR) between the original and the reconstructed image is introduced.

$$\mathrm{PSNR}(f, f^{'}) = 10 \log \frac{255^2}{\left(\frac{1}{MN}\right) \sum_{n=1}^{N} \sum_{m=1}^{M} [f(m,n) - f^{'}(m,n)]^2}$$

$f(m,n)$ Value of an original image

$f^{'}(m,n)$ Value of decryption image

The analysis of security and robustness

Robustness of the encryption image to occlusion and noise

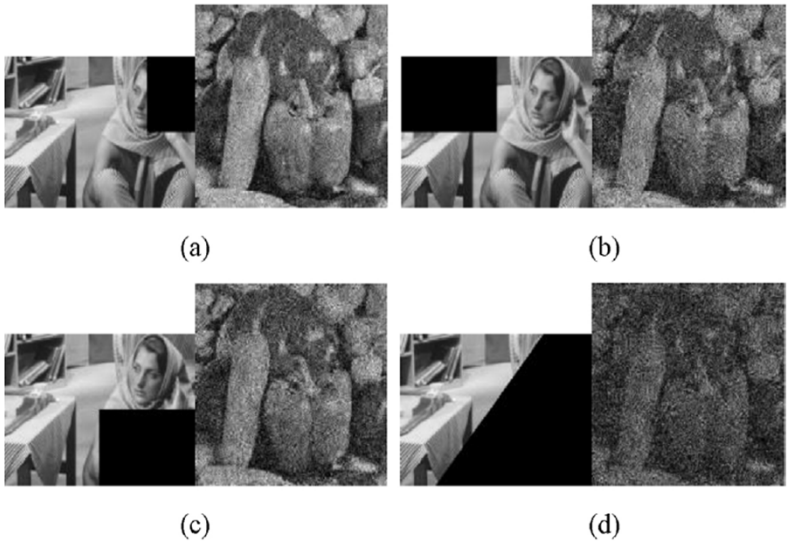

Fig. 7. The analysis of robustness to the pixels occluded of the fused image. (a) 1/8 pixels occluded, PSNR=16.0305 dB; (b) ¼ pixels occluded (upper left), PSNR= 12.7756 dB; (c) ¼ pixels occluded (lower right), PSNR= 12.9857 dB; (d) ½ pixels occluded, PSNR= 9.1114 dB.

Robustness to noise

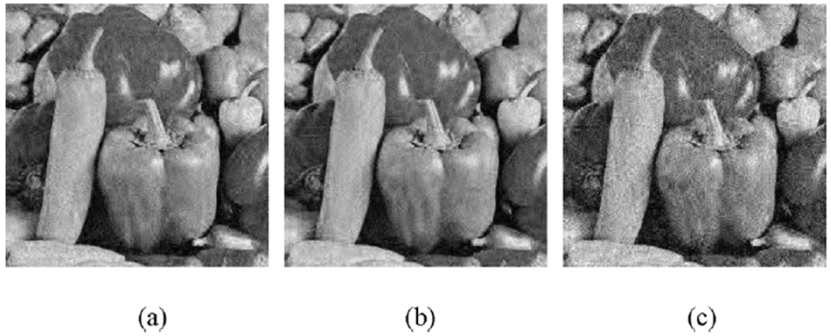

Fig. 8. Reconstruction images under various noise conditions. (a) Add Gausian white noise of mean 0 and variance 0.1, PSNR= 23.7422 dB; (b) add salt and pepper with 0.05 density to the encryption image, PSNR= 24.6522 dB; (c) add salt and pepper with 0.10 density to the encryption image, PSNR= 20.0274 dB.

Robustness to Wrong Key

Robustness to wrong key

- The multi-encryption method has high security and robustness.
- As shown in Fig. 7, the decryption images are very sensitive to the correct keys.
- If and only if all the keys are available, the correct decrypted image can be obtained.
- If the cipher attackers want to decipher the secret information by using exhaustive attacks, they can impossibly achieve.
- The method has stronger resistance against the exhaustive attacks, which can guarantee the security of information more effectively.

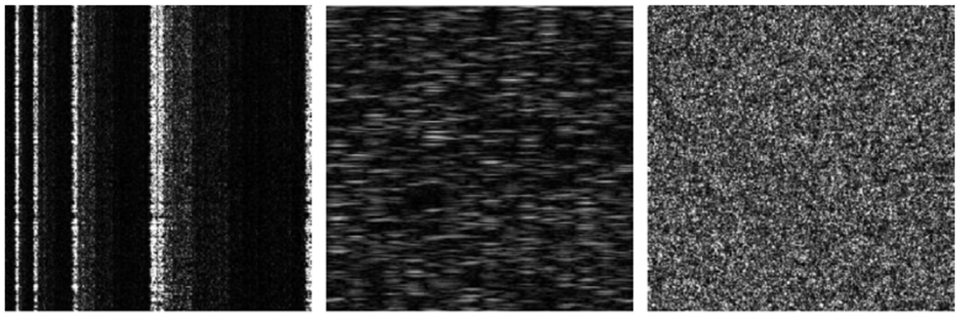

Fig. 9. Decryption image using wrong keys (a) using wrong key 1, PSNR= 2.4874 dB; (b) using wrong key 2, PSNR= 1.715 dB; (c) using wrong key 3, PSNR= 3.4262 dB.

Thank You